Cisco VPN Client User Guide for Linux and Solaris

Release 3.7

Corporate Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

Customer Order Number:
Text Part Number: OL-3272-01

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

CCIP, the Cisco Arrow logo, the Cisco *Powered* Network mark, the Cisco Systems Verified logo, Cisco Unity, Follow Me Browsing, FormShare, iQ Breakthrough, iQ Expertise, iQ FastTrack, the iQ Logo, iQ Net Readiness Scorecard, Networking Academy, ScriptShare, SMARTnet, TransPath, and Voice LAN are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn, Discover All That's Possible, The Fastest Way to Increase Your Internet Quotient, and iQuick Study are service marks of Cisco Systems, Inc.; and Aironet, ASIST, BPX, Catalyst, CCDA, CCDP, CCIE, CCNA, CCNP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, the Cisco IOS logo, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Empowering the Internet Generation, Enterprise/Solver, EtherChannel, EtherSwitch, Fast Step, GigaStack, Internet Quotient, IOS, IP/TV, LightStream, MGX, MICA, the Networkers logo, Network Registrar, *Packet*, PIX, Post-Routing, Pre-Routing, RateMUX, Registrar, SlideCast, StrataView Plus, Stratm, SwitchProbe, TeleRouter, and VCO are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and certain other countries.

All other trademarks mentioned in this document or Web site are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0208R)

Cisco VPN Client User Guide for Linux and Solaris
Copyright © 2002, Cisco Systems, Inc.
All rights reserved.

CONTENTS

About This Guide vii

- Audience vii
- Contents vii
- Related Documentation viii
- Terminology viii
- Document Conventions viii
  - Data Formats ix
- Obtaining Documentation ix
  - World Wide Web ix
  - Documentation CD-ROM ix
  - Ordering Documentation ix
  - Documentation Feedback x
- Obtaining Technical Assistance x
  - Cisco.com x
  - Technical Assistance Center xi
    - Cisco TAC Web Site xi
    - Cisco TAC Escalation Center xi

CHAPTER 1 **Introduction to the VPN Client** 1-1

- VPN Client Overview 1-1
- VPN Client Features 1-2
  - Main Features 1-2
  - Program Features 1-3
  - IPSec Features 1-4
    - IPSec Attributes 1-4
  - Authentication Features 1-5

CHAPTER 2 **Installing the VPN Client** 2-1

- Uninstalling an Old Client 2-1
  - Uninstalling a VPN Client for Solaris 2-1
  - Uninstalling a VPN Client for Linux 2-2
- System Requirements 2-2
  - Linux System Requirements 2-2
    - Firewall Issues 2-2

Troubleshooting Tip 2-2
Solaris System Requirements 2-3
Changing a Kernel Version 2-3
Unpacking the VPN Client Files 2-4
Installing the Software 2-4
Installing the VPN Client for Linux 2-4
VPN Client for Linux Install Script Notes 2-5
Installing the VPN Client for Solaris 2-5
VPN Client for Solaris Install Script Notes 2-6

CHAPTER 3 **User Profiles 3-1**
Sample Profile Description 3-1
Modifying the Sample Profile 3-2
Creating a User Profile 3-2

CHAPTER 4 **Using the Command-Line Interface 4-1**
Displaying a List of Commands 4-1
Establishing a Connection 4-1
Authentication Prompts 4-2
Rekeying Issues 4-3
DNS Server Settings 4-3
Disconnecting the VPN Client 4-3
Displaying VPN Client Statistics 4-3
Examples 4-4
No Options 4-4
Reset Option 4-5
Traffic Option 4-5
Tunnel Option 4-5
Route Option 4-5
Event Logging 4-6
Enabling Logging 4-6
Viewing Log Files 4-6
Client Auto Update Messages 4-7

CHAPTER 5 **Managing Digital Certificates 5-1**
Setting Certificate Keywords 5-1
Certificate Command Syntax 5-1
Certificate Contents 5-2

Certificate Passwords **5-3**
Certificate Tags **5-4**
Certificate Management Operations **5-4**
Enrolling Certificates **5-6**
Enrollment Operations **5-6**
Enrollment Troubleshooting Tip **5-7**

INDEX

About This Guide

This guide describes how to install, use, and manage the Cisco VPN Client for the following operating systems:

- Linux for Intel
- Solaris UltraSPARC

Audience

This guide is for remote clients who want to set up virtual private network (VPN) connections to a central site. Network administrators can also use this guide for information about configuring and managing VPN connections for remote clients. You should be familiar with UNIX platforms and know how to use UNIX applications. Network administrators should be familiar with UNIX system configuration and management and know how to install, configure, and manage internetworking systems.

Contents

This guide contains the following chapters:

- Chapter 1, “Introduction to the VPN Client.” This chapter provides a brief introduction to the VPN client software.
- Chapter 2, “Installing the VPN Client.” This chapter describes how to install the VPN client software on your workstation.
- Chapter 3, “User Profiles.” This chapter describes how to set up user profiles for connection entries.
- Chapter 4, “Using the Command-Line Interface.” This chapter describes the command-line interface and lists the commands and their descriptions.
- Chapter 5, “Managing Digital Certificates.” This chapter describes how to manage your digital certificate stores.
- Index

Related Documentation

The following is a list of user guides and other documentation related to the VPN client for Linuxand Solaris and the VPN devices that provide the connection to the private network. Cisco VPN Client User Guide for Mac OS X

- *Release Notes for the Cisco VPN Client, Version 3.7 for Linux, Solaris, and Mac OS X*
- *Cisco VPN Client Administrator Guide*
- *Cisco VPN 3000 Series Concentrator Series Getting Started Guide*
- *Cisco VPN 3000 Series Concentrator Reference Volume I: Configuration*
- *Cisco VPN 3000 Series Concentrator Reference Volume II: Administration and Monitoring*

Terminology

In this user guide:

- The term *Cisco VPN device* refers to the following Cisco products:
  - Cisco IOS devices that support Easy VPN server functionality
  - VPN 3000 Series Concentrators
  - Cisco PIX Firewall Series
- The term *PC* refers generically to any personal computer.

Document Conventions

This guide uses the following typographic conventions:

- **Boldface** font—Describes user actions and commands.
- *Italic* font—Describes arguments that you supply the values for.
- `Screen` font—Describes terminal sessions and information displayed by the system.
- **`Boldface screen`** font—Describes information that you must enter.

Note Means *reader take note*. Notes contain helpful suggestions or references to material not covered in the manual.

Caution Means *reader be careful*. In this situation, you might do something that could result in equipment damage or loss of data.

Data Formats

When you configure the VPN client, enter data in these formats unless the instructions indicate otherwise.

- IP Address—Use standard 4-byte dotted decimal notation (for example, 192.168.12.34). You can omit leading zeros in a byte position.
- Host names—Use legitimate network host or end-system name notation (for example, VPN01). Spaces are not allowed. A host name must uniquely identify a specific system on a network. A host name can be up to 255 characters in length.
- User names and Passwords—Text strings for user names and passwords use alphanumeric characters in both upper- and lower case. Most text strings are case sensitive. For example, simon and Simon would represent two different user names. The maximum length of user names and passwords is generally 32 characters, unless specified otherwise.

Obtaining Documentation

These sections explain how to obtain documentation from Cisco Systems.

World Wide Web

You can access the most current Cisco documentation on the World Wide Web at this URL:

http://www.cisco.com

Translated documentation is available at this URL:

http://www.cisco.com/public/countries_languages.shtml

Documentation CD-ROM

Cisco documentation and additional literature are available in a Cisco Documentation CD-ROM package, which is shipped with your product. The Documentation CD-ROM is updated monthly and may be more current than printed documentation. The CD-ROM package is available as a single unit or through an annual subscription.

Ordering Documentation

You can order Cisco documentation in these ways:

- Registered Cisco.com users (Cisco direct customers) can order Cisco product documentation from the Networking Products MarketPlace:

  http://www.cisco.com/cgi-bin/order/order_root.pl

- Registered Cisco.com users can order the Documentation CD-ROM through the online Subscription Store:

  http://www.cisco.com/go/subscription

- Nonregistered Cisco.com users can order documentation through a local account representative by calling Cisco Systems Corporate Headquarters (California, U.S.A.) at 408 526-7208 or, elsewhere in North America, by calling 800 553-NETS (6387).

Documentation Feedback

You can submit comments electronically on Cisco.com. In the Cisco Documentation home page, click the **Fax** or **Email** option in the "Leave Feedback" section at the bottom of the page.

You can e-mail your comments to bug-doc@cisco.com.

You can submit your comments by mail by using the response card behind the front cover of your document or by writing to the following address:

Cisco Systems
Attn: Document Resource Connection
170 West Tasman Drive
San Jose, CA 95134-9883

We appreciate your comments.

Obtaining Technical Assistance

Cisco provides Cisco.com as a starting point for all technical assistance. Customers and partners can obtain online documentation, troubleshooting tips, and sample configurations from online tools by using the Cisco Technical Assistance Center (TAC) Web Site. Cisco.com registered users have complete access to the technical support resources on the Cisco TAC Web Site.

Cisco.com

Cisco.com is the foundation of a suite of interactive, networked services that provides immediate, open access to Cisco information, networking solutions, services, programs, and resources at any time, from anywhere in the world.

Cisco.com is a highly integrated Internet application and a powerful, easy-to-use tool that provides a broad range of features and services to help you with these tasks:

- Streamline business processes and improve productivity
- Resolve technical issues with online support
- Download and test software packages
- Order Cisco learning materials and merchandise
- Register for online skill assessment, training, and certification programs

If you want to obtain customized information and service, you can self-register on Cisco.com. To access Cisco.com, go to this URL:

http://www.cisco.com

Technical Assistance Center

The Cisco Technical Assistance Center (TAC) is available to all customers who need technical assistance with a Cisco product, technology, or solution. Two levels of support are available: the Cisco TAC Web Site and the Cisco TAC Escalation Center.

Cisco TAC inquiries are categorized according to the urgency of the issue:

- Priority level 4 (P4)—You need information or assistance concerning Cisco product capabilities, product installation, or basic product configuration.
- Priority level 3 (P3)—Your network performance is degraded. Network functionality is noticeably impaired, but most business operations continue.
- Priority level 2 (P2)—Your production network is severely degraded, affecting significant aspects of business operations. No workaround is available.
- Priority level 1 (P1)—Your production network is down, and a critical impact to business operations will occur if service is not restored quickly. No workaround is available.

The Cisco TAC resource that you choose is based on the priority of the problem and the conditions of service contracts, when applicable.

Cisco TAC Web Site

You can use the Cisco TAC Web Site to resolve P3 and P4 issues yourself, saving both cost and time. The site provides around-the-clock access to online tools, knowledge bases, and software. To access the Cisco TAC Web Site, go to this URL:

http://www.cisco.com/tac

All customers, partners, and resellers who have a valid Cisco service contract have complete access to the technical support resources on the Cisco TAC Web Site. The Cisco TAC Web Site requires a Cisco.com login ID and password. If you have a valid service contract but do not have a login ID or password, go to this URL to register:

http://www.cisco.com/register/

If you are a Cisco.com registered user, and you cannot resolve your technical issues by using the Cisco TAC Web Site, you can open a case online by using the TAC Case Open tool at this URL:

http://www.cisco.com/tac/caseopen

If you have Internet access, we recommend that you open P3 and P4 cases through the Cisco TAC Web Site.

Cisco TAC Escalation Center

The Cisco TAC Escalation Center addresses priority level 1 or priority level 2 issues. These classifications are assigned when severe network degradation significantly impacts business operations. When you contact the TAC Escalation Center with a P1 or P2 problem, a Cisco TAC engineer automatically opens a case.

To obtain a directory of toll-free Cisco TAC telephone numbers for your country, go to this URL:

http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml

Before calling, please check with your network operations center to determine the level of Cisco support services to which your company is entitled: for example, SMARTnet, SMARTnet Onsite, or Network Supported Accounts (NSA). When you call the center, please have available your service agreement number and your product serial number.

CHAPTER 1

Introduction to the VPN Client

The Cisco VPN Client is a software application that runs on computers using any of the following operating systems:

- Linux for Intel—RedHat Version 6.2 or later, or compatible libraries with glibc Version 2.1.1-6 or later, using kernel Versions 2.2.12 or later.
- Solaris UltraSPARC—32-bit or 64-bit Solaris kernel OS Version 2.6 or later.

The VPN client on a remote PC, communicating with a Cisco VPN device on an enterprise network or with a service provider, creates a secure connection over the Internet. This connection allows you to access a private network as if you were an on-site user, creating a virtual private network (VPN).

The following VPN devices can terminate VPN connections from VPN clients:

- Cisco IOS devices that support Easy VPN server functionality
- VPN 3000 Series Concentrators
- Cisco PIX Firewall Series

Use the VPN client command-line interface to establish a VPN connection to a private network, manage connection entries, certificates, and events logging.

This chapter contains the following sections:

- VPN Client Overview, page 1-1
- VPN Client Features, page 1-2

VPN Client Overview

The VPN client works with a Cisco VPN device to create a secure connection, called a tunnel, between your computer and a private network. It uses Internet Key Exchange (IKE) and IP Security (IPSec) tunneling protocols to establish and manage the secure connection.

The steps used to establish a VPN connection can include:

- Negotiating tunnel parameters (addresses, algorithms, lifetime)
- Establishing VPN tunnels according to the parameters
- Authenticating users (from usernames, group names and passwords, and X.509 digital certificates)
- Establishing user access rights (hours of access, connection time, allowed destinations, allowed protocols)

- Managing security keys for encryption and decryption
- Authenticating, encrypting, and decrypting data through the tunnel

For example, to use a remote PC to read e-mail at your organization, the connection process might be similar to the following:

1. Connect to the Internet.
2. Start the VPN client.
3. Establish a secure connection through the Internet to your organization's private network.
4. When you open your e-mail

   The Cisco VPN device

   – Uses IPSec to encrypt the e-mail message

   – Transmits the message through the tunnel to your VPN client

   The VPN client

   – Decrypts the message so you can read it on your remote PC

   – Uses IPSec to process and return the message to the private network through the Cisco VPN device

VPN Client Features

The tables in the following sections describe the VPN client features.

Main Features

This section describes the main features of the VPN client. Table 1-1 lists the VPN client main features.

Table 1-1 Main Features

Features	Description
Operating Systems	• Linux (Intel) • Solaris (UltraSPARC-32 and 64 bit)
Connection types	• async serial PPP • Internet-attached Ethernet **Note** The VPN client supports only one PPP and one Ethernet adapter.
Protocol	IP

Table 1-1 Main Features (continued)

Features	Description
Tunnel protocol	IPSec
User Authentication	• RADIUS • RSA SecurID • VPN server internal user list • PKI digital certificates • NT Domain (Windows NT)

Program Features

The VPN client supports the program features listed in Table 1-2.

Table 1-2 Program Features

Program Feature	Description
Servers Supported	• Cisco IOS devices that support Easy VPN server functionality • VPN 3000 Series Concentrators • Cisco PIX Firewall Series
Local LAN access	The ability to access resources on a local LAN while connected through a secure gateway to a central-site VPN server (if the central site grants permission).
Automatic VPN client configuration option	The ability to import a configuration file.
Event logging	The VPN client log collects events for viewing and analysis.
NAT Transparency (NAT-T)	Enables the VPN client and the VPN device to automatically detect when to use IPSec over UDP to work properly in port address translation (PAT) environments.
Update of centrally controlled backup server list	The VPN client learns the backup VPN server list when the connection is established. This feature is configured on the VPN device and pushed to the VPN client. The backup servers for each connection entry are listed on the Backup Servers tab.
Set MTU size	The VPN client automatically sets a size that is optimal for your environment. However, you can also set the MTU size manually. For information on adjusting the MTU size, see the *Cisco VPN Client Administrator Guide*.
Support for Dynamic DNS (DDNS host name population)	The VPN client sends its host name to the VPN device when the connection is established. If this occurs, the VPN device can send the host name in a DHCP request. This causes the DNS server to update its database to include the new host name and VPN client address.

IPSec Features

The VPN client supports the IPSec features listed in Table 1-3.

Table 1-3 IPSec Features

IPSec Feature	Description
Tunnel Protocol	IPSec
Transparent tunneling	• IPSec over UDP for NAT and PAT • IPSec over TCP for NAT and PAT
Key Management protocol	Internet Key Exchange (IKE)
IKE Keepalives	A tool for monitoring the continued presence of a peer and reporting the VPN client's continued presence to the peer. This lets the VPN client notify you when the peer is no longer present. Another type of keepalives keeps NAT ports alive.
Split tunneling	The ability to simultaneously direct packets over the Internet in clear text and encrypted through an IPSec tunnel. The VPN device supplies a list of networks to the VPN client for tunneled traffic. You enable split tunneling on the VPN client and configure the network list on the VPN device.
Support for Split DNS	The ability to direct DNS packets in clear text over the Internet to domains served through an external DNS (serving your ISP) or through an IPSec tunnel to domains served by the corporate DNS. The VPN server supplies a list of domains to the VPN client for tunneling packets to destinations in the private network. For example, a query for a packet destined for corporate.com would go through the tunnel to the DNS that serves the private network, while a query for a packet destined for myfavoritesearch.com would be handled by the ISP's DNS. This feature is configured on the VPN server (VPN concentrator) and enabled on the VPN client by default. To use Split DNS, you must also have split tunneling configured.

IPSec Attributes

The VPN client supports the IPSec attributes listed in Table 1-4.

Table 1-4 IPSec Attributes

IPSec Attribute	Description
Main Mode and Aggressive Mode	Ways to negotiate phase 1 of establishing ISAKMP Security Associations (SAs)
Authentication algorithms	• HMAC (Hashed Message Authentication Coding) with MD5 (Message Digest 5) hash function • HMAC with SHA-1 (Secure Hash Algorithm) hash function
Authentication Modes	• Preshared Keys • X.509 Digital Certificates

Table 1-4 IPSec Attributes (continued)

IPSec Attribute	Description
Diffie-Hellman Groups	• 1 • 2
Encryption algorithms	• 56-bit DES (Data Encryption Standard) • 168-bit Triple-DES • AES 128-bit and 256-bit
Extended Authentication (XAUTH)	The capability of authenticating a user within IKE. This authentication is in addition to the normal IKE phase 1 authentication, where the IPSec devices authenticate each other. The extended authentication exchange within IKE does not replace the existing IKE authentication.
Mode Configuration	Also known as ISAKMP Configuration Method
Tunnel Encapsulation Modes	• IPSec over UDP (NAT/PAT) • IPSec over TCP (NAT/PAT)
IP compression (IPCOMP) using LZS	Data compression algorithm

Authentication Features

The VPN client supports the authentication features listed in Table 1-5.

Table 1-5 Authentication Features

Authentication Feature	Description
User authentication through VPN central-site device	• Internal through the VPN device's database • RADIUS • NT Domain (Windows NT) • RSA (formerly SDI) SecurID or SoftID
Certificate Management	Allows you to manage the certificates in the certificate stores.
Certificate Authorities (CAs)	CAs that support PKI SCEP enrollment.
Ability to authenticate using smart cards	Physical SecurID cards or keychain fobs for passcode generation.
Peer Certificate Distinguished Name Verification	Prevents a VPN client from connecting to an invalid gateway by using a stolen but valid certificate and a hijacked IP address. If the attempt to verify the domain name of the peer certificate fails, the VPN client connection also fails.

Installing the VPN Client

This chapter describes how to install the VPN client software on your workstation, and includes the following sections:

- Uninstalling an Old Client, page 2-1
- System Requirements, page 2-2
- Unpacking the VPN Client Files, page 2-4
- Installing the Software, page 2-4

You should be familiar with software installation on UNIX computers to perform this procedure.

The VPN client consists of:

- A driver, which is a loadable module.
- A set of commands accessible through your shell, which is used to access the applications.

The commands and some parts of the driver are distributed in binary form only.

Uninstalling an Old Client

This section describes how to uninstall the VPN client.

- You *must* uninstall an old VPN client for Solaris before you install a new VPN client.
- You are *not required* to uninstall an old VPN client for Linux before you install a new VPN client.
- You must uninstall any VPN 5000 client before you install a VPN client. Refer to the Cisco VPN 5000 Client documentation for more information.

Uninstalling a VPN Client for Solaris

If a VPN client for Solaris was previously installed, you must remove the old VPN client before you install a new one.

To uninstall a package, use the **pkgrm** command. For example:

```
pkgrm vpnclient
```

Uninstalling a VPN Client for Linux

To uninstall the VPN client for Linux:

1. Locate the script vpn_uninstall.

   This file must be run as root.

2. You are prompted to remove all profiles and certificates.
   - If you answer yes, all binaries, startup scripts, certificates, profiles, and any directories that were created during the installation process are removed.
   - If you answer no, all binaries and startup scripts are removed, but certificates, profiles, and the vpnclient.ini file remain.

System Requirements

This section describes system requirements for the VPN client for each operating system.

Linux System Requirements

The VPN client for Linux supports Red Hat Version 6.2 Linux (Intel), or compatible libraries with glibc Version 2.1.1-6 or later, using kernel Versions 2.2.12 or later.

Note The VPN client for Linux does not support kernel Version 2.5 or SMP (multiprocessor) kernels.

Firewall Issues

If you are running a Linux firewall (for example, ipchains or iptables), be sure that the following types of traffic are allowed to pass through:

- UDP port 500
- UDP port 10000 (or any other port number being used for IPSec/UDP)
- IP protocol 50 (ESP)
- TCP port configured for IPSec/TCP
- NAT-T port 4500

Troubleshooting Tip

The following two lines might be added by default with your Linux installation in the /etc/sysconfig/ipchains directory. For Redhat, this might be written to the /etc/sysconfig/ipchains directory. These two commands might prevent UDP traffic from passing through.

```
-A input -p udp -s 0/0 -d 0/0 0:1023 -j REJECT
-A input -p udp -s 0/0 -d 0/0 2049 -j REJECT
```

If you have problems with UDP traffic, try one of the following solutions:

- First delete the above two reject lines, then enter the following two commands:

```
/etc/init.d/ipchains stop
/etc/init.d/ipchains start
```

Note The ipchains might be replaced by iptables or it might be located in a different directory on your Linux distribution.

- Add the following rule to the default ipchains firewall configuration, or add it above any UDP reject line.

  ```
  -A input -p udp -s 0/0 -d 0/0 500 -j ACCEPT
  ```

  This rule allows UDP port 500, which is required for the VPN client connection.

Solaris System Requirements

The VPN client for Solaris runs on any UltraSPARC computer running a 32-bit or 64-bit Solaris kernel OS Version 2.6 or later.

Changing a Kernel Version

You can install the VPN client running the 32-bit or 64-bit version of the kernel (referred to as 32-bit mode and 64-bit mode). If you experience problems installing or running the VPN client in one mode, try the other one.

To see which mode the system is running in, enter this command:

```
isainfo -kv
```

If the cipsec module is loaded correctly, the dmesg log displays a message similar to the following:

```
Oct 29 11:09:54 sol-2062 cipsec: [ID 952494 kern.notice] Cisco Unity IPSec Module Load OK
```

Note If the dmesg log does not show the cipsec log message, you should switch to the other mode.

To switch to 32-bit mode:

- Temporarily—Enter the following command (ok is the system prompt):

  ```
  ok boot kernel/unix
  ```

- Permanently—Enter the following command as root, then restart your computer:

  ```
  eeprom boot-file=/platform/sun4u/kernel/unix
  ```

To switch to 64-bit mode:

- Temporarily—Enter the following command (ok is the system prompt):

  ```
  ok boot kernel/sparcv9/unix
  ```

- Permanently—Enter the following command as root, then restart your computer:

  ```
  eeprom boot-file=/platform/sun4u/kernel/sparcv9/unix
  ```

Unpacking the VPN Client Files

The VPN client is shipped as a compressed tar file.

To unpack the files

Step 1 Download the packed files, either from your internal network or the Cisco website, to a directory of your choice.

Step 2 Copy the VPN client file to a selected directory.

Step 3 Unpack the file using the **zcat** and **tar** commands.

For example, the command for Linux is:

```
zcat vpnclient-linux-3.7.xxx-K9.tar.gz | tar xvf -
```

The command for Solaris is:

```
zcat vpnclient-solaris-3.7.xxx-K9.tar.Z | tar xvf -
```

This command creates the vpnclient directory in the current directory.

Installing the Software

The following sections describe the installation procedure for the VPN client for each operating system.

Installing the VPN Client for Linux

Before you install a new version of the VPN client, or before you reinstall your current version, you must use the **stop** command to disable VPN service.

If you are upgrading from the VPN 5000 client to the VPN client, use the following **stop** command:

```
/etc/rc.d/init.d/vpn stop
```

If you are upgrading from the VPN 3000 client to the VPN client, use the following **stop** command:

```
/etc/rc.d/init.d/vpnclient_init stop
```

To install the VPN client for Linux

Step 1 Obtain superuser privileges to run the install script.

Step 2 Enter the following commands:

```
cd vpnclient
./vpn_install
```

The default directories for the binaries, kernel, VPN modules, and profiles are listed during the installation process.

You receive the following prompts during the installation:

- Directory where binaries will be installed [/lib/modules/<kernel version>/build/]
- Automatically start the VPN service at boot time [yes]

- Directory containing linux kernel source code [/usr/src/linux]
- Is the above correct [y]

Step 3 Press **Enter** to choose the default response. At the directory prompts, if you do not choose the default, you must enter another directory in your user's path.

Step 4 If the installer cannot autodetect these settings, you might receive the following prompts:

- Directory containing init scripts:
  - The directory where scripts that are run at boot time are kept. Typically this is /etc/init.d or /etc/rc.d/init.d
- Directory containing run level directories (rcX.d):
  - The directory that contains init's run level directories. Typically this is /etc or /etc/rc.d

Step 5 Enable the VPN service by using one of the following methods:

- Restart your computer.
- Enable the service without restarting. Enter the following command:

```
/etc/rc.d/init.d/vpnclient_init start
```

VPN Client for Linux Install Script Notes

During the installation process:

1. The module is compiled, linked, and copied to either the directory /lib/modules/preferred/CiscoVPN, if it exists, or to /lib/modules/*system*/CiscoVPN, where *system* is the kernel version.
2. The application binaries are copied to the specified destination directory.
3. The startup file /etc/rc.d/init.d/vpnclient_init is created to enable and disable the VPN service.
4. The links /etc/rc3.d/s85vpnclient and /etc/rc5.d/s85vpnclient are added to run level 3 and level 5 if startup at boot time is requested.

   These links allow the tunnel server to start at boot time and run in levels 3 and 5.

Installing the VPN Client for Solaris

Before you install a new version of the VPN client, or before you reinstall your current version, you must uninstall the old VPN client. See the "Uninstalling an Old Client" section on page 2-1 for more information.

Note If you are installing the VPN Client for Solaris, Release 3.7 or later on a Version 2.6 Solaris platform, you receive the following message during the VPN client installation: "Patch 105181 version 29 (or higher) to Solaris 2.6 is required for the client to function properly. Installing without this patch will cause the kernel to crash as soon as the client kernel module is loaded. This patch is available from Sun as part of the "Recommended Solaris Patch Cluster". If you proceed with installation, the kernel module will not be enabled. After you have installed the patch, you may enable the kernel module by uncommenting all lines in /etc/iu.ap that contain 'cipsec'."

To install the VPN client for Solaris

Step 1 Obtain superuser privileges to run the install script.

Step 2 Enter the following command:

```
pkgadd -d . vpnclient
```

The default directories for the binaries, kernel, VPN modules, and profiles are listed during the installation process.

You receive the following prompts during the installation:

- Directory where binaries will be installed [/usr/local/bin]
- Is the above correct [y]
- If the installer finds a conflict with the VPN client files and another application, you receive this message:

  The following files are already installed on the system and are being used by another package:<installer lists files> Do you want to install these conflicting files [y,n,?,q]
- The following files are being installed with setuid and/or setgid permissions:<installer lists files>Do you want to install these as setuid/setgid files [y,n,?,q]
- This package contains scripts which will be executed with super-user permission during the process of installing this package. Do you want to continue with the installation of <vpnclient> [y,n,?]

Step 3 Press **Enter** to choose the default response. At the directory prompts, if you do not choose the default, you must enter another directory in your user's path.

Step 4 Restart your computer.

VPN Client for Solaris Install Script Notes

During the installation process:

1. The following line is added to the /etc/iu.ap file to enable the autopush facility at startup:

   ```
   <dev_name> -1 0 cipsec
   ```

   where dev_name is the name of the interface without the trailing numbers (for example ipdtp, le, or hme). A line is added for every supported network device detected.
2. The VPN module is copied to the /kernel/strmod directory, which is in the system's module search path.

The **pkginfo** command provides information about the installed packages. For more information on other package-related commands, enter:

```
man pkgadd
```

CHAPTER 3

User Profiles

The VPN client uses parameters that must be uniquely configured for each remote user of the private network. Together these parameters make up a user profile, which is contained in a profile configuration file (.pcf file). User profiles reside in the default directory /etc/CiscoSystemsVPNClient/Profiles/, or in the directory specified during the VPN client installation.

User profile parameters include the remote server address, IPSec group name and password, use of a log file, use of backup servers, and automatic connect upon startup. Each connection entry has its own user profile.

Tip User profiles for the VPN client are interchangeable between platforms.

This chapter describes how to create a VPN client user profile and includes the following sections:

- Sample Profile Description, page 3-1
- Modifying the Sample Profile, page 3-2
- Creating a User Profile, page 3-2

To set global profiles for all users, refer to the *Cisco VPN Client Administrator Guide*.

Sample Profile Description

There are two ways to create a user profile:

- Use a text editor to modify the sample profile that comes with the VPN client installer and rename it.
- Create a unique user profile using a text editor.

There is only one user profile per connection.

The VPN client software is shipped with a sample user profile. The file is named sample.pcf.

The following is an example of a sample user profile that might be shipped with your installer.

```
[main]
Description=sample user profile
Host=10.7.44.1
AuthType=1
GroupName=monkeys
EnableISPConnect=0
ISPConnectType=0
ISPConnect=
ISPCommand=
```

```
Username=gawf
SaveUserPassword=0
EnableBackup=0
BackupServer=
EnableNat=0
CertStore=0
CertName=
CertPath=
CertSubjectName=
CertSerialHash=00000000000000000000000000000000
DHGroup=2
ForceKeepAlives=0
```

Modifying the Sample Profile

To modify the sample profile

Step 1 Using a text editor, open the sample user profile.

Step 2 Modify the keywords you want to change.

See your administrator for IP addresses, user name, and any security information.

Step 3 Save your new profile with a unique name in the /etc/CiscoSystemsVPNClient/Profiles/ directory.

When you use the **vpnclient connect** command to establish a connection, use your new profilename.

Creating a User Profile

You can create your own user profile from scratch by using any text editing program.

At a minimum, you need the following keywords listed in your profile:

- [main]
- Host
- AuthType
- GroupName
- Username

Save your new profile in the /etc/CiscoSystemsVPNClient/Profiles/ directory. See your administrator for IP addresses, user names, and any security information.

Table 3-1 describes keywords that can be in a user profile. User profile keywords are not case sensitive unless indicated in the description.

Table 3-1 User Profile Keywords

Keywords	Description
[main]	A required keyword that identifies the main section. Enter exactly as shown as the first entry in the user profile.
Description = *String*	This optional keyword describes this user profile. The maximum length is 246 alphanumeric characters.
Host = *IP_Address or hostname*	The hostname or IP address of the VPN device you want to connect with. The maximum length of the hostname is 255 alphanumeric characters.
AuthType = **{ 1 | 3 }**	The authentication type that this user is using. • **1** is preshared keys. • **3** is a digital certificate using an RSA signature. If you select **AuthType 1**, you must also configure the **GroupName** and **GroupPwd**.
GroupName = *String*	The name of the IPSec group configured on the VPN device that contains this user. The maximum length is 32 alphanumeric characters. This keyword is case sensitive.
GroupPwd = *String*	The password for the IPSec group that contains this user. The minimum length is 4 alphanumeric characters. The maximum is 32. This keyword is case sensitive and entered in clear text.
encGroupPwd = *String*	Displays the group password in the user profile in its encrypted form. It is binary data represented as alphanumeric text.
Username = *String*	The name that identifies a user as a valid member of the IPSec group specified in **GroupName**. The VPN client prompts the user for this value during user authentication. The maximum length is 32 alphanumeric characters. This keyword is case sensitive and entered in clear text.
UserPassword = *String*	This password is used during extended authentication. • If **SaveUserPassword** is enabled, the first time the VPN client reads this password, it is saved in the user profile as **encUserPassword**, and the clear text version is deleted. • If **SaveUserPassword** is disabled, the VPN client deletes the clear text version of the user password in the user profile but it does not create an encrypted version.
encUserPassword = *String*	Displays the user password in the user profile in its encrypted form. It is binary data represented as alphanumeric text.
SaveUserPassword = **{ 0 | 1 }**	Determines if the user password or its encrypted form are valid in the user profile. • **0**, the default, displays the user password in clear text in the user profile and is saved locally. • **1** displays the user password in the user profile in its encrypted version, and the password is not saved locally. This value is set in the VPN device, not in the VPN client.

Table 3-1 User Profile Keywords (continued)

Keywords	Description
EnableBackup = **{ 0 | 1 }**	Specifies to use a backup server if the primary server is not available. • **0**, the default, disables the backup server. • **1** enables the backup server. You must also specify a **BackupServer**.
BackupServer = *IP_Address or hostname*	List of IP addresses or hostnames of backup servers. Separate multiple entries by commas. The maximum length of hostname is 255 alphanumeric characters.
EnableLocalLAN = **{ 0 | 1 }**	Allows you to configure access to your local LAN. • **0**, the default, disables local LAN access. • **1** enables local LAN access.
EnableNAT = **{ 0 | 1 }**	Specifies whether or not to enable secure transmission between a VPN client and a VPN device through a router serving as a firewall, which might also be using the NAT protocol. • **0**, the default, disables IPSec through NAT mode. • **1** enables IPSec through NAT mode.
TunnelingMode = **{ 0 | 1 }**	Allows you to select which form of NAT transversal is used. • **0**, the default, specifies IPSec over UDP for NAT transparency. • **1** specifies IPSec over TCP for NAT transparency. You must also have IPSec through NAT enabled.
TCPTunnelingPort = **{ 0 | 65535 }**	Sets which TCP port to use for the cTCP protocol. The default is 10000. You must also have IPSec through NAT enabled and the Tunneling Mode set for IPSec over TCP.
ForceKeepAlives = **{ 0 | 1 }**	Allows the VPN client to keep sending IKE and ESP keepalives for a connection at approximately 20-second intervals so that the port on an ESP-aware NAT/Firewall does not close. • **0**, the default, disables keepalives. • **1** enables keepalives.
PeerTimeout = *Number*	The number of seconds to wait before terminating a connection when the VPN device on the other end of the tunnel is not responding. The range is 30 to 480 seconds. The default is 90.
CertStore = **{ 0 | 1 }**	Identifies the type of store containing the configured certificate. • **0** = default, none. • **1** = Cisco.
CertName = *String*	Identifies the certificate used to connect to the VPN device. The maximum length is 129 alphanumeric characters.
CertPath = *String*	The path name of the directory containing the certificate file. The maximum length is 259 alphanumeric characters.

Table 3-1 User Profile Keywords (continued)

Keywords	Description
CertSubjectName = *String*	The qualified Distinguished Name (DN) of the certificate's owner. You can either *not* include this keyword in the user profile, or leave this entry blank.
CertSerialHash = *String*	A hash of the certificate's complete contents, which provides a means of validating the authenticity of the certificate. You can either *not* include this keyword in the user profile, or leave this entry blank.
DHGroup = **{ 1 | 2 }**	Allows a network administrator to override the configured group value used to generate Diffie-Hellman key pairs on a VPN device. • **1** = modp group 1 • **2** = modp group 2 The default is 2. The VPN Concentrator configuration for IKE Proposal must match the DHGroup in the VPN client. If the AuthType is set to 3 (digital certificate), this keyword has no effect on the VPN client.

CHAPTER 4

Using the Command-Line Interface

This chapter describes common operations using the command-line interface and contains the following sections:

- Displaying a List of Commands, page 4-1
- Establishing a Connection, page 4-1
- Disconnecting the VPN Client, page 4-3
- Displaying VPN Client Statistics, page 4-3
- Event Logging, page 4-6

Displaying a List of Commands

To display a list of available VPN client commands, locate the directory that contains the VPN client software and enter the **vpnclient** command at the command line prompt.

The following example shows the command and the information that is displayed:

```
%vpnclient
Cisco Systems VPN Client Version 3.7 (Rel)
Copyright (C) 1998-2002 Cisco Systems, Inc. All Rights Reserved.
Client Type(s): Linux
Running on: Linux 2.4.18-3 #1 Thu Apr 18 07:37:53 EDT 2002 i686

Usage:
  vpnclient connect <profile> [user <username>] [eraseuserpwd | pwd
<password>] [nocertpwd]
  vpnclient disconnect
  vpnclient stat [reset] [traffic] [tunnel] [route] [repeat]
  vpnclient notify
```

Establishing a Connection

This section describes how to establish a VPN connection using the **vpnclient connect** command and optional command parameters.

Note If you are connecting to a VPN device by using Telnet or SSH, check to see if the device allows split tunneling. If it does not, you lose connectivity to your VPN device after making a VPN connection.

To establish a connection, enter the following command:

```
vpnclient connect <profile> [user <username>] [eraseuserpwd | pwd <password>] [nocertpwd]
```

The parameters for the **vpnclient connect** command are described in Table 4-2.

Table 4-1 Parameters for the vpnclient connect Command

Parameter	Description
<**profile**> (required)	The name of the user profile configured for this connection entry (.pcf file). Enter the profile name without the .pcf file extension. If your profile name contains spaces, enclose it in double quotation marks on the command line.
user <**username**> (optional)	The username configured for this connection entry. If you use this option with the **pwd** option, the username prompt is surpressed in authentication dialog box.
{ eraseuserpassword | pwd <**password**> **}** (optional)	• **eraseuserpassword** erases the user password that is saved on the VPN client workstation, forcing the VPN client to prompt you for a password each time you establish a connection. • **pwd** <**password**> surpresses the password prompt in the authentication dialog box.
nocertpwd (optional)	Suppresses the prompt for a certificate password and assumes that the password is blank. If you use this option, you cannot set a password for your certificate. For more information, see the "Certificate Passwords" section on page 5-3.

Note If your user profile is configured with the **SaveUserPassword** keyword set to the default, the password is saved locally.

For more information on profiles, see Chapter 3, "User Profiles.".

Authentication Prompts

Depending on the parameters that have been configured in your user profile, you are prompted for the following passwords:

- Group password
- User name
- User password
- Certificate password

If your VPN client has been configured to use SecurID or RADIUS authentication, you are also prompted for those passwords.

See your administrator for any security information.

Rekeying Issues

When the connection is established, the VPN Client window stays in the foreground to allow the VPN client to be reauthenticated during a rekey by the VPN device. To send the VPN client window to the background, press **Ctrl-Z** and enter the **bg** command at the command line prompt.

If the VPN device you are connecting to is configured to support rekeying and you send the VPN client window to the background, the tunnel disconnects when the first rekey occurs.

The VPN client responds to rekey triggers based on *time*, not *data*. If you want VPN client connections rekeyed, you must configure the concentrator so that the IKE proposal is set to rekey every 1800 seconds and IPSec parameters are set to rekey every 600 seconds.

DNS Server Settings

You can configure the concentrator to send the IP addresses of DNS servers to the VPN client to use during tunnel sessions.

If the client receives the DNS server settings, it copies the file /etc/resolv.conf to a backup file /etc/resolv.conf.vpnbackup. When the tunnel closes, the original contents of /etc/resolv.conf are restored.

Note Refer to the configuration guide for your VPN device for information on DNS server settings.

Disconnecting the VPN Client

This section describes methods for disconnecting the VPN client.

To disconnect from your session, use one of the following methods:

- Enter the following command:

  ```
  vpnclient disconnect
  ```

  The following example shows the command that disconnects you from your secure connection and the prompt that appears when you are not connected.

  ```
  vpnclient disconnect
  Disconnecting the IPSEC link.
  Your IPSec link is not connected.
  ```

- Press **Crtl-C** while you are in the VPN Client window.

Displaying VPN Client Statistics

This section describes the VPN client statistics command **vpnclient stat** and its optional parameters.

To generate status information about your connection, enter the following command:

```
vpnclient stat [reset][traffic][tunnel][route][repeat]
```

If you enter this command without any of the optional parameters, the **vpnclient stat** command displays all status information. The optional parameters are described in Table 4-2.

Table 4-2 Optional Parameters for the vpnclient stat Command

Parameter	Description
reset	Restarts all connection counts from zero.
traffic	Displays a summary of bytes in and out, packets encrypted and decrypted, and packets bypassed and discarded.
tunnel	Displays IPSec tunneling information.
route	Displays configured routes.
repeat	Provides a continuous display, refreshing it every few seconds. To end the display, press **Ctrl-C**.

Examples

This section shows examples of output from the different options for the **vpnclient stat** command.

No Options

The following is a sample output from the **vpnclient stat** command with no options.

```
vpnclient stat

IPSec tunnel information.
Client address: 209.154.64.50
Server address: 10.10.32.32
Encryption: 168-bit 3-DES
Authentication: HMAC-MD5
IP Compression: None
NAT passthrough is active on port 5000

VPN traffic summary.
Time connected: 0 day<s>, 00:18.32
Bytes out: 3420
Bytes in: 3538
Packets encrypted: 23
Packets decrypted: 57
Packets bypassed: 102
Packets discarded: 988

Configured routes
Secured   Network Destination    Netmask           Bytes
   *       10.10.32.32          255.255.255.255       7638
   *       0.0.0.0              0.0.0.0               1899
```

Reset Option

To reset all connection counters, use the **vpnclient stat reset** command.

```
vpnclient stat reset
Tunnel statistics have been reset.
```

Traffic Option

The following is a sample output from the **vpnclient stat** command with the traffic option.

```
vpnclient stat traffic

VPN traffic summary
Time connected: 0 day<s>, 00:30:04
Bytes out: 5460
Bytes in: 6090
Packets encrypted: 39
Packets decrypted: 91
Packets bypassed: 159
Packets discarded: 1608
```

Tunnel Option

The following is a sample output from the **vpnclient stat** command with the tunnel option. The **vpnclient stat tunnel** command shows only tunneling information.

```
vpnclient stat tunnel

IPSec tunnel information.
Client address: 220.111.22.30
Server address: 10.10.10.1
Encryption: 168-bit 3-DES
Authentication: HMAC-MD5
IP Compression: None
NAT passthrough is active on port 5000
```

Route Option

The following is a sample output from the **vpnclient stat** command with the route option.

```
vpnclient stat route

Configured routes
Secured   Network Destination    Netmask           Bytes
   *       10.10.02.02          255.255.255.255       17638
   *       0.0.0.0              0.0.0.0               18998
```

Event Logging

This section provides information on event logging, including how to capture and view logging information.

Enabling Logging

You must be a system administrator or have access to the global profile (vpnclient.ini) to enable logging. The global profile, located in /etc/CiscoSystemsVPNClient/vpnclient.ini, must include the following parameters:

```
[main]
EnableLog=1
[LOG.IKE]
LogLevel=3
[LOG.CM]
LogLevel=3
[LOG.PPP]
LogLevel=3
[LOG.CVPND]
LogLevel=3
[LOG.CERT]
LogLevel=3
[LOG.IPSEC]
LogLevel=3
```

For more information about the global profile, refer to the *Cisco VPN Client Administrator Guide*.

Viewing Log Files

To view logging information, enter the following command:

```
/usr/local/bin/ipseclog /directory/clientlog.txt
```

Note If you did not use the default directory /usr/local/bin during installation, you must enter logging commands using your chosen path.

To view logging information in real time, enter the following command after you start the ipseclog:

```
tail -f /directory/clientlog.txt
```

The ipseclog does not automatically go to the background. To send the ipseclog to the background, press **Ctrl-Z** and enter the **bg** on the command line, or enter the ampersand symbol (&) at the end of the **view** command, as shown in the following example:

```
/usr/local/bin/ipseclog /directory/clientlog.txt &
```

If the ipseclog is in the background, you must send it to the foreground before you end the VPN client application. To send the ipseclog to the foreground, enter **fg** on the command line.

Client Auto Update Messages

When the VPN client receives an auto-update notification from the VPN remote access device, it logs the notification, but takes no further action. The message logged upon receipt of an auto-update message has the following format:

```
688 10:14:23.811 08/08/2001 Sev=Info/4 IKE/0x4300005B^M CLIENT_UPDATE_NOTIFICATION: Client
Type=”linux” Revisions=”3.0.5” URL=”tftp://x:/y/z”
```

To receive auto-update messages and other notifications from the network administrator, use the **vpnclient notify** command.

CHAPTER 5

Managing Digital Certificates

This chapter describes how to manage digital certificates in your certificate store for the Cisco VPN client by using the command-line interface. Your certificate store is the location in your local file system for storing digital certificates. The store for the VPN client is the Cisco store.

This chapter includes the following sections:

- Setting Certificate Keywords, page 5-1
- Certificate Command Syntax, page 5-1
- Certificate Contents, page 5-2
- Certificate Passwords, page 5-3
- Certificate Tags, page 5-4
- Certificate Management Operations, page 5-4
- Enrolling Certificates, page 5-6

Setting Certificate Keywords

To use certificates for authentication, you must correctly set all keywords that apply to certificates in your user profile. Check your settings for the following keywords:

- **AuthType = 3** (certificate authentication)
- **CertStore = 1** (Cisco certificate store)
- **CertName = Common Name** (This must be the same common name that is entered for a certificate.)

See Chapter 3, “User Profiles,” for more information on setting parameters in your user profile.

Certificate Command Syntax

Digital certificate management is implemented using the command line interface.

The command line interface for certificate management operates in two ways:

- The standard UNIX shell at which you enter all arguments for a given command on the same line.

  cisco_cert_mgr -U -op enroll -f *filename* **-chall** *challenge_phrase*

- A prompting mode in which you enter minimum arguments for a given command and are prompted for any remaining information.

  The minimum command line argument follows this basic form:

  ```
  cisco_cert_mgr -U -op operation
  cisco_cert_mgr -R -op operation
  cisco_cert_mgr -E -op operation
  ```

  Where:

  – **-U** applies to the user or private certificate.

    You can use the -U flag for all certificate management command operations, except enroll_resume.

  – **-R** applies to the root certificate or certificate authority (CA) certificate.

    You can use the -R flag for list, view, verify, delete, export, import, and change password operations.

  – **-E** applies to certificate enrollment.

    You can only use the -E flag with list and delete, and you must specify it using the enroll_resume operation.

The operation for the specified certificate follows the **-op** argument. Valid operations for the certificate manager command are list, view, verify, delete, export, import, enroll, enroll_file, and enroll_resume. For more information on these operations, see the "Certificate Management Operations" section on page 5-4.

Certificate Contents

This section describes the type of information contained in a digital certificate.

A typical digital certificate contains the following information:

- Common name—The name of the owner, usually both the first and last names. This field identifies the owner within the Public Key Infrastructure (PKI) organization.
- Department—The name of the owner's department. This is the same as the organizational unit.
  – If you are connecting to a VPN 3000 concentrator, this field must match the **Group Name** configured for the owner in the concentrator.
  – If you are connecting to a VPN 5000 concentrator, this field must match the **VPNGroup-*groupname*** configured in the concentrator.
- Company—The company in which the owner is using the certificate. This is the same as the organization.
- State—The state in which the owner is using the certificate.
- Country—The two-character country code in which the owner's system is located.
- Email—The e-mail address of the owner of the certificate.
- Thumbprint—An MD5 hash of the certificate's complete contents. The thumbprint provides a means for validating the authenticity of the certificate. For example, if you contact the issuing CA, you can use this identifier to verify that this certificate is the correct one to use.
- Key size—The size of the signing key pair in bits.

- Subject—The fully qualified domain name (FQDN) of the certificate's owner. This field uniquely identifies the owner of the certificate in a format that can be used for LDAP and X.500 directory queries. A typical subject includes the following fields:
  - common name (**cn**)
  - organizational unit, or department (**ou**)
  - organization or company (**o**)
  - locality, city, or town (**l**)
  - state or province (**st)**
  - country (**c)**
  - e-mail address (**e)**

  Other items might be included in the Subject, depending on the certificate.
- Serial number—A unique identifier used for tracking the validity of the certificate on the certificate revocation lists (CRLs).
- Issuer—The FQDN of the source that provided the certificate.
- Not before—The beginning date that the certificate is valid.
- Not after—The end date beyond which the certificate is no longer valid.

The following output is an example of the type of information contained in a digital certificate:

```
Common Name: Fred Flinstone
Department: Rock yard
Company: Stone Co.
State: (null)
Country: (null)
Email: fredf@stonemail.fake
Thumb Print: 2936A0C874141273761B7F06F8152CF6
Key Size: 1024
Subject:e=fredf@stonemail.fake,cn=Fred Flinstone,ou=Rockyard,o=Stone Co. l=Bedrock
Serial #: 7E813E99B9E0F48077BF995AA8D4ED98
Issuer: Stone Co.
Not before: Thu May 24 18:00:00 2001
Not after: Mon May 24 17:59:59 2004
```

Certificate Passwords

Each digital certificate is protected by a password. Many operations performed by the certificate management command require that you enter the password before the operation can take place.

The operations that require you to enter a password are:

- Delete
- Import
- Export
- Enroll

Note For the enroll operation, the password to protect the digital certificate is a separate password from the optional challenge password that you enter for the server certificate.

You are prompted for any passwords that are required to complete the command. You must enter the password and verify the password again before the command can execute. If the password is not accepted, you must re-enter the command.

When you establish a VPN connection with a certificate, a certificate password is also required.

All passwords can be up to 32 alphanumeric characters in length, and are case sensitive.

Certificate Tags

A certificate tag is the identifier for each unique certificate. Each certificate added to the certificate store is assigned a certificate tag. An enroll operation also generates a certificate tag, even if the enroll operation does not complete.

Some certificate management operations require that you enter a certificate tag argument before the operation can take place. Operations that require certificate tags are listed in Table 5-1. Use the **list** operation to find your certificate tag.

To enter a certificate tag argument, use the **-ct** command followed by the certificate identifier, listed as **-ct** ***Cert #*** next to the operation.

The following example shows the **view** command with a required certificate tag:

```
cisco_cert_mgr -U -op view -ct 0
```

Where the operation is **view**, and the certificate tag is **0**.

If you do not enter the **-ct** argument and certificate tag, the command line prompts you for them. If you enter an invalid certificate tag, the command line lists all certificates in the certificate store, and prompts you again for the certificate tag.

Certificate Management Operations

List all certificate management operations on the command line following the minimum command line argument. Valid operation strings allow you to list, view, verify, delete, export, import, and enroll digital certificates in your store.

The following is an example of a certificate management command with the **list** operation, and a sample output.

```
cisco_cert_mgr -U -op list

cisco_cert_mgr Version 3.0.7

        Cert #          Common Name
          0             Fred Flinstone
          1             Dino
```

Table 5-1 describes the operations that can be used with the certificate management command.

Table 5-1 Parameters for the cert_mgr Command

Parameter	Description
list	Lists all certificates in the certificate store. Each certificate in the list is identified by a unique certificate tag (*Cert #)*.
view -ct *Cert #*	Views the specified certificate. You must enter a certificate tag.

Table 5-1 Parameters for the cert_mgr Command (continued)

Parameter	Description
verify -ct *Cert #*	Verifies that the specified certificate is valid. You must enter a certificate tag. If the certificate is verified, the message 'Certificate *Cert #* verified' appears. If the certificate fails verification for any reason, the message 'Certificate *Cert #* failed verification' appears. Following this message is a text string which describes the reason for the failure.
delete -ct *Cert #*	Deletes the specified certificate. You must enter a certificate tag.
export -ct *Cert #* **-f** *filename*	Exports the identified certificate from the certificate store to a specified file. You must enter a certificate tag and a filename. If either is omitted, the command line prompts you for them. You must enter the full path of the destination. If you enter only the filename, the file is placed in your working directory.
import -f *filename*	Imports a certificate from a specified file to the certificate store. This operation requires two different passwords: the password that protects the file (assigned by your administrator), and the password you select to protect the certificate.
enroll **-cn** *common_name* **-ou** *organizational_unit* **-o** *organization* **-st** *state* **-c** *country* **-e** *email* **-ip** *IP_Address* **-dn** *domain_name* **-caurl** *url_of _CA* **-cadn** *domain_name* **[-chall** *challenge_phrase***]**	For user certificates only. Obtains a certificate by enrolling you with a Certificate Authority (CA) over the network. Enter each keyword individually on the command line. See the "Enrolling Certificates" section on page 5-6 for more information. You can obtain a challenge phrase from your administrator or from the CA.
enroll_file **-cn** *common_name* **-ou** *organizational_unit* **-o** *organization* **-st** *state* **-c** *country* **-e** *email* **-ip** *IP_Address* **-dn** *domain_name* **-f** *filename* **-enc [base64 | binary]**	For user certificates only. Generates an enrollment request file that can be e-mailed to the CA or pasted into a webpage form. When the certificate is generated by the CA, you must import it using the **import** operation. See the "Enrolling Certificates" section on page 5-6 for more information.

Table 5-1 Parameters for the cert_mgr Command (continued)

Parameter	Description
enroll_resume -E -ct *Cert #*	This operation cannot be used with user or root certificates. Resumes an interrupted network enrollment. You must enter the **-E** argument and a certificate tag.
changepassword -ct *Cert #*	Changes a password for a specified digital certificate. You must enter a certificate tag. You must enter the current password before you select the new password and confirm it.

Enrolling Certificates

A Certificate Authority (CA) is a trusted organization that issues digital certificates to users to provide a means for verifying that users are who they claim to be. The certificate enrollment operations allow you to obtain your certificate from a CA over the network or from an enrollment request file.

There are three types of certificate enrollment operations.

- The **enroll** operation allows you to obtain a certificate by enrolling with a CA over the network. You must enter the URL of the CA, the domain name of the CA, and the common name.
- The **enroll_file** operation generates an enrollment request file that you can e-mail to a CA or post into a webpage form. You must enter a filename, a common name, and the encoding type you want to use.

  With the enroll and enroll_file operations, you can include additional information with associated keywords. These keywords are described in Table 5-2.
- The **enroll_resume** operation resumes an interrupted network enrollment. You must enter the **-E** argument and a certificate tag. To find your certificate tag, use the **list** operation.

Enrollment Operations

To use enrollment operations, enter the certificate manager command and the enroll operation you want to use with the associated keywords on the command line.

- The following example shows the enroll command with the minimum required keywords for common name (-cn), URL of the CA (-caurl) and domain name of the CA (-cadn):

  ```
  cisco_cert_mgr -U -op enroll -cn Ren Hoek -caurl
  http://172.168.0.32/certsrv/mscep/mscep.dll -cadn nobody.fake
  ```

- The following example shows the enroll_file command with the minimum required keywords for filename (-f), common name (-cn), and encoding type (-enc):

  ```
  cisco_cert_mgr -U -op enroll_file -f filename -cn Ren Hoek -enc base64
  ```

- The following example shows the enroll_file command with the required minimum arguments and additional keywords:

```
cisco_cert_mgr -U -op enroll_file -f filename -cn Ren Hoek -ou Customer Service -o
Stimpy, Inc, -st CO -c US -e ren@fake.fake -ip 10.10.10.10 -dn fake.fake -enc binary
```

- The following example shows the enroll_resume command:

```
cisco_cert_mgr -E -op enroll_resume -ct 4
```

Table 5-2 describes options for the enroll, enroll_file, and enroll_resume operations.

Table 5-2 Keywords for Enrollment Operations

Parameter	Description
-cn *common_name*	The common name for the certificate.
-ou *organizational_unit*	The organizational unit for the certificate.
-o *organization*	The organization for the certificate.
-st *state*	The state for the certificate.
-c *country*	The country for the certificate.
-e *email*	The user e-mail address for the certificate.
-ip *IP_Address*	The IP address of the user's system.
-dn *domain_name*	The FQDN of the user's system.
-caurl *url_of_CA*	The URL or network address of the CA.
-cadn *domain_name*	The CA's domain name.
[-chall *challenge_phrase* **]**	You can obtain the challenge phrase from your administrator or from the CA.
-enc [base64 | binary]	Select encoding of the output file. The default is base64. • **base64** is an ASCII-encoded PKCS10 file that you can display because it is in a text format. Choose this type when you want to cut and paste the text into the CA's website. • **binary** is a base-2 PKCS10 (Public-Key Cryptography Standards) file. You cannot display a binary-encoded file.

Enrollment Troubleshooting Tip

If the enrollment request for a user certificate, using either the enroll or enroll_file operation, generates a CA certificate instead of a user certificate, the CA might be overwriting some of the distinguished naming information. This might be caused by a configuration issue on the CA, or a limitation of how the CA responds to enrollment requests.

The common name and subject information in the enrollment request must match the certificate generated by the CA for the VPN client to recognize it as the same user certificate that was requested. If it does not match, the VPN client does not install the new user certificate as the user certificate it had requested.

To check for this problem, view the enrollment request on the VPN client and compare the common name and subject lines with a view of the certificate from the CA. If they do not match, then the CA is overwriting information from the client request.

To work around this issue, use the invalid certificate as an example and create an enrollment request that matches the output of the CA certificate.

Note If the CA's certificate contains multiple department (mulitple ou fields), you can add multiple departments to the VPN client enrollment request by using the plus sign (+) between the department fields.

INDEX

A

aggressive mode **1-4**
algorithms
  authentication **1-4**
  data compression **1-5**
  encryption **1-5**
authentication
  algorithms **1-4**
  extended **1-5**
  features **1-5**
  mode **1-4**
  type **3-3**

B

backup server **3-4**
batch files
  erasing saved password **4-2**

C

certificate
  contents **5-2**
  distinguished name **3-5**
  enrolling a CA **5-6**
  enrollment **5-2**
  example **5-3**
  hash of contents **3-5**
  management **5-1**
  management operations **5-4**
  name **3-4**
  passwords **5-3**
  path name **3-4**
  peer **1-5**
  root **5-2**
  store **3-4, 5-1**
  tags **5-4**
  user **5-2**
change password operation **5-6**
command-line interface
  connect **3-2**
  disconnect **4-3**
  displaying commands **4-1**
  logging **4-6**
  minimum argument **5-2**
  notify **4-7**
  stat **4-3**
commands
  tar **2-4**
  zcat **2-4**
connection types **1-2**

D

data compression **1-5**
data formats **ix**
delete operation **5-5**
DHCP request **1-3**
Diffie-Hellman groups **1-5**
disconnecting the VPN client **4-3**
displaying available commands **4-1**
DNS server **1-3**
documentation
  conventions **viii**
  related **viii**

E

enabling VPN service **2-5**
encrypt group password **3-3**
encryption algorithm **1-5**
encrypt user password **3-3**
enroll file operation **5-5**
enrolling a CA for certificates **5-2, 5-6**
enrollment keywords **5-7**
enroll operation **5-5**
enroll resume operation **5-6**
eraseuserpwd parameter **4-2**
ESP keepalives **3-4**
export operation **5-5**
extended authentication **1-5**

F

features
  authentication **1-5**
  IPSec **1-4**
  program **1-3**
  VPN Client **1-2**
FQDN (fully qualified domain name) **5-3**

G

group name **3-3**
group password **3-3**

H

hash **3-5, 5-2**
host name **1-3, 3-3**

I

IKE keepalives **1-4, 3-4**
IKE protocols **1-1**
import operation **5-5**
installer contents **2-1**
install script
  Linux **2-5**
  Solaris **2-6**
introduction **1-1**
IP chains **2-3**
IP protocol **1-2**
IPSec
  attributes **1-4**
  features **1-4**
  through NAT **3-4**
IPSec group
  name **3-3**
  password **3-3**

K

keepalives **1-4, 3-4**
kernel version
  changing **2-3**
  requirements **2-2**
key size **5-2**
keywords for enrollment operations **5-7**

L

libraries **2-2**
list operation **5-4**
local LAN access **1-3, 3-4**
logging commands **4-6**

M

main mode **1-4**
mode
  aggressive **1-4**

authentication **1-4**
configuration **1-5**
main **1-4**
NAT **3-4**
tunnel encapsulation **1-5**
MTU size **1-3**

N

NAT mode **3-4**
NAT transparency **3-4**
NAT transversal **3-4**
notify command **4-7**

O

operations for certificate management **5-4**

P

password
group **3-3**
IPSec group **3-3**
overriding **4-2**
string **3-3**
user profile **3-3**
peer certificate **1-5**
peer timeout **3-4**
ports
TCP **3-4**
profiles **3-1**
program features **1-3**
protocols
DHCP **1-3**
IKE **1-1**
IP **1-2**
PPP **1-2**
TCP **3-4**
UDP **1-3, 2-3**

R

Red Hat Software **2-2**
root certificates **5-2**

S

save user password **3-3**
shared keys
authentication type **3-3**
Diffie-Hellman group **3-5**
smart cards **1-5**
split DNS **1-4**
split tunneling **1-4**
statistics **4-3**
supported VPN devices **1-1**
system requirements **2-2**

T

tar command **2-4**
TCP protocol **3-4**
terminate connections **1-1**
transparent tunneling **1-4**
tunneling
encapsulation mode **1-5**
protocol **1-3**
split **1-4**

U

UDP protocol **1-3**
UltraSPARC computer **2-3**
uninstalling an old client **2-1**
unpacking the VPN client files **2-4**
user authentication **1-3, 1-5**

user certificates **5-2**
user name **3-3**
user password **3-3**
user profiles
  certificate
    keywords **5-1**
  creating **3-2**
  described **3-1**
  example **3-1**
  location **3-1**
  parameters **3-3**

V

verify operation **5-5**
viewing the logging files **4-6**
view operation **5-4**
VPN Client
  defined **1-1**
  features **1-2**
vpnclient connect command **3-2**
vpnclient disconnect command **4-3**
vpnclient stat command **4-3**
VPN devices **1-1**

X

X.509 certificates **1-1**
XAUTH (extended authentication) **1-5**

Z

zcat command **2-4**